
Advisory:
Google Chrome Carriage Return Null Object Memory Exhaustion Remote Dos.

Version Affected:
Chrome/0.2.149.30
Chrome/0.2.149.29

Release Date:
Disclosed: 22 September 2008
Release Date. September 23 ,2008

Description:
The Google chrome browser is vulnerable to memory exhaustion based denial of service which can be triggered remotely.The vulnerability triggers when Carriage Return(\r\n\r\n) is passed as an argument to window.open() function. It makes the Google Chrome to generate number of windows at the same time thereby leading to memory exhaustion. The behavior can be easily checked by looking at the task manager as with no time the memory usage rises high. The problem lies in the handling of object and its value returned by the javascript function. Once it is triggered the pop ups are started generating. The Google Chrome browser generate object windows continuously there by affecting memory of the resultant system. Probably it can be crashed wihin no time. User interaction is required in this.

Proof-of-Concept:
Click Here

Credit:
Aditya K Sood (Team Lead, www.EvilFingers.com)

Disclaimer:
The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There is no representation or warranties, either express or implied by or with respect to anything in this document, and shall not be liable for a ny implied warranties of merchantability or fitness for a particular purpose or for any indirect special or consequential damages.
